Claims

1. A data processing apparatus for processing content data provided by a recording or communication medium, characterized in that said apparatus comprises:

a cryptography process section for executing a cryptography process on said content data; and

a control section for executing control for said cryptography process section, and

said cryptography process section:

is configured to generate partial integrity check values as integrity check values for a partial data set containing one or more partial data obtained by a content data-constituting section into a plurality of parts, and to collate the generated integrity check values to verify said partial data, and

generates an intermediate integrity check value based on a partial integrity check value set data string containing at least one or more of said partial integrity check values, and uses the generated intermediate integrity check value to verify the entirety of the plurality of partial data sets corresponding to the plurality of partial integrity check values constituting said partial integrity check value set.

2. The data processing apparatus according to Claim 1, characterized in that:

said partial integrity check value is generated by means of a cryptography process with a partial-check-value-generating key applied thereto, using partial data to be checked, as a message,

said intermediate integrity check value is generated by means of a cryptography process with an general-check-value-generating key applied thereto, using a partial integrity check value set data string to be checked, as a message, and

said cryptography process section is configured to store said partial-integrity-check-value-generating value and said general-integrity-check-value-generating key.

3. The data processing apparatus according to Claim 1, characterized in that: said cryptography process has plural types of partial-check-value-generating key corresponding to generated partial integrity check values.

4. The data processing apparatus according to Claim 2, characterized in that:

said cryptography process is a DES cryptography process, and

said cryptography process section is configured to execute the DES cryptography process.

5. The data processing apparatus according to Claim 2, characterized in that:

said partial integrity check value is a message authentication code (MAC) generated in an DES-CBC mode using partial data to be checked, as a message,

said intermediate value is a message authentication code (MAC) generated in a DES-CBC mode using a partial integrity check value set data string to be checked, as a message, and

said cryptography process section is configured to execute the cryptography process in the DES-CBS mode.

6. The data processing apparatus according to Claim 5, characterized in that: in the DES-CBC mode-based cryptography process configuration of said cryptography process section, Triple DES is applied only in part of a message string to be processed.

7. The data processing apparatus according to Claim 1, characterized in that:

said data processing apparatus has a signature key, and

said cryptography process section: is configured to apply a value generated from said intermediate value by means of said signature key-applied cryptography process as a collation value for data verification.

8. The data processing apparatus according to Claim 7, characterized in that:

said data processing apparatus has a plurality of different signature keys as signature keys, and

said cryptography process section: is configured to apply one of said plurality of different signature keys which is selected depending on a localization of said content data, to the cryptography process for said intermediate integrity check value to obtain the collation value for data verification.

9. The data processing apparatus according to Claim 8, characterized in that: said data processing apparatus has a common signature key common to all entities of a system for executing a data verifying process and an apparatus-specific signature key specific to each apparatus that executes a data verifying process.

10. The data processing apparatus according to Claim 1, characterized in that:

said partial integrity check value contains one or more header section integrity check values generated for intra-header-section data partly constituting data and one or more content integrity check values generated for content block data partly constituting the data, and

said cryptography process is configured to generate one or more header section integrity check values for a partial data set in said intra-header-section data to execute a collation process, generate one or more content integrity check values for a partial

data set in said intra-content-section data to execute a collation process, and further generate a general integrity check value based on all said header section integrity check values and said content integrity check values generated, to execute a collation process in order to verify the data.

11. The data processing apparatus according to Claim 1, characterized in that:

said partial integrity check value contains one or more header section integrity check values generated for intra-header-section data partly constituting data, and

said cryptography process is configured to generate one or more header section integrity check values for a partial data set in said intra-header-section data to execute a collation process and further generate a general integrity check value based on said one or more header section integrity check values generated and on content block data constituting part of said data, to execute a collation process in order to verify the data.

12. The data processing apparatus according to Claim 1, characterized by further comprising: a recording device for storing data validated by said cryptography process section.

13. The data processing apparatus according to Claim 12, characterized in that:

said control section is configured so that if in the process executed by said cryptography process section to collate the partial integrity check value, the collation is not established, and

said control section suspends the process for storing data in said recording device.

14. The data processing apparatus according to Claim 1, characterized by further comprising: a reproduction process section for reproducing data validated by said cryptography process section.

15. The data processing apparatus according to Claim 14, characterized in that:

if in the process executed by said cryptography process section to collate the partial integrity check value, the collation is not established, and

said control section suspends the reproduction process in said reproduction process section.

16. The data processing apparatus according to Claim 14, characterized by comprising: control means for collating only the header section integrity check values in the data during the process executed by said cryptography process section to collate the partial integrity check values and transmitting data for which

collation of the header section integrity check values has been established, to said reproduction process section for reproduction.

17. A data processing apparatus for processing content data provided by a recording or communication medium, characterized in that said apparatus comprises:

a cryptography process section for executing a cryptography process on said content data; and

a control section for executing control for said cryptography process section, and

said cryptography process section: is configured to generate, if data to be verified are encrypted, integrity check values for the data to be verified by means of a signature data-applied cryptography process from data on arithmetic operation results obtained by executing an arithmetic operation process on decrypted data obtained by executing a decryption process on the encrypted data.

18. The data processing apparatus according to Claim 17, characterized in that: said arithmetic operation process comprises performing an exclusive-OR operation on decrypted data every predetermined bytes, the decrypted data being obtained by decrypting said encrypted data.

19. A data processing method for processing content data provided by a recording or communication medium, characterized in that said method:

generates partial integrity check values as integrity check values for a partial data set containing one or more partial data obtained by a content data constituting section into a plurality of parts, and collates the generated integrity check values to verify said partial data, and

generates an intermediate integrity check value based on a partial integrity check value set data string containing at least one or more of said partial integrity check values, and uses the generated intermediate integrity check value to verify the entirety of the plurality of partial data sets corresponding to the plurality of partial integrity check values constituting said partial integrity check value set.

20. The data processing method according to Claim 19, characterized in that:

said partial integrity check value is generated by means of a cryptography process with a partial-check-value-generating key applied thereto, using partial data to be checked, as a message, and

said intermediate integrity check value is generated by means of a cryptography process with an general-check-value-generating

key applied thereto, using a partial integrity check value set data string to be checked, as a message.

21. The data processing method according to Claim 20, characterized in that: said partial integrity check value is generated by applying different types of partial-check-value-generating keys corresponding to generated partial integrity check values.

22. The data processing method according to Claim 20, characterized in that: said cryptography process is a DES cryptography process.

23. The data processing method according to Claim 19, characterized in that:

said partial integrity check value is a message authentication code (MAC) generated in a DES-CBC mode using partial data to be checked, as a message, and

said intermediate value is a message authentication code (MAC) generated in a DES-CBC mode using a partial integrity check value set data string to be checked, as a message.

24. The data processing method according to Claim 19, characterized in that: a value generated from said intermediate

value by means of a signature key-applied cryptography process is applied as a collation value for data verification.

25. The data processing method according to Claim 24, characterized in that: different signature keys are applied to the cryptography process for said intermediate integrity check value depending on a localization of said content data, to obtain the collation value for data verification.

26. The data processing method according to Claim 25, characterized in that: a common signature key common to all entities of a system for executing a data verifying process or an apparatus-specific signature key specific to each apparatus that executes a data verifying process is selected and used as said signature key depending on the localization of the content data.

27. The data processing method according to Claim 19, characterized in that:

said partial integrity check value contains one or more header section integrity check values generated for intra-header-section data partly constituting data and one or more content integrity check values generated for intra-content-section data partly constituting the data, and

a data verifying process:

generates one or more header section integrity check values for a partial data set in said intra-header-section data to execute a collation process;

generates one or more content integrity check values for a partial data set in said intra-content-section data to execute a collation process; and

further generates a general integrity check value based on all said header section integrity check values and said content integrity check values generated, to execute a collation process in order to verify the data.

28. The data processing method according to Claim 19, characterized in that:

said partial integrity check value contains one or more header section integrity check values generated for intra-header-section data partly constituting data, and

the data verifying process:

generates one or more header section integrity check values for a partial data set in said intra-header-section data to execute a collation process; and

further generates a general integrity check value based on said one or more header section integrity check values generated and on content block data constituting part of said data, to execute a collation process in order to verify the data.

29. The data processing method according to Claim 19, characterized by further comprising: a process for storing, after data verification, storing validated data.

30. The data processing method according to Claim 29, characterized in that: if in the process for collating said partial integrity check value, the collation is not established, control is executed such as to suspend the process for storing data in said recording device.

31. The data processing method according to Claim 19, characterized by further comprising: a data reproduction process for reproducing data after the data verification.

32. The data processing method according to Claim 31, characterized in that:

if in the process for collating said partial integrity check value, the collation is not established, and

control is executed such as to suspend the reproduction process executed in said reproduction process section.

33. The data processing method according to Claim 31, characterized in that said method:

collates only the header section integrity check values in the data during the process for collating the partial integrity

check values and transmits data for which collation of the header section integrity check values has been established, to said reproduction process section for reproduction.

34. The data processing method for processing content data provided by a recording or communication medium, the method being characterized in that said method:

if data to be verified are encrypted, executes an arithmetic operation process on decrypted data obtained by decrypting the encrypted data,

executes a signature key-applied cryptography process on data on arithmetic operation results obtained by said arithmetic operation, to generate integrity check values for said data to be verified.

35. The data processing method according to Claim 34, characterized in that: said arithmetic operation process comprises performing an exclusive-OR operation on decrypted data every predetermined bytes, the decrypted data being obtained by decrypting said encrypted data.

36. A data verifying value imparting method for a data verifying process, characterized in that said method:

imparts partial integrity check values as integrity check values for a partial data set containing one or more partial data

obtained by a content data constituting section into a plurality of parts, and

imparts to data to verified, an intermediate integrity check value used to verify a partial integrity check value set data string containing at least one or more of said partial integrity check values.

37. The data verifying value imparting method according to Claim 36, characterized in that:

said partial integrity check value is generated by means of a cryptography process with a partial-check-value-generating key applied thereto, using partial data to be checked, as a message, and

said intermediate integrity check value is generated by means of a cryptography process with an general-check-value-generating key applied thereto, using a partial integrity check value set data string to be checked, as a message.

38. The data verifying value imparting method according to Claim 37, characterized in that: said partial integrity check value is generated by applying different types of partial-check-value-generating keys corresponding to generated partial integrity check values.

39. The data verifying value imparting method according to Claim 37, characterized in that: said cryptography process is a DES cryptography process.

40. The data verifying value imparting method according to Claim 36, characterized in that:

said partial integrity check value is a message authentication code (MAC) generated in a DES-CBC mode using partial data to be checked, as a message, and

said intermediate value is a message authentication code (MAC) generated in a DES-CBC mode using a partial integrity check value set data string to be checked, as a message.

41. The data verifying value imparting method according to Claim 36, characterized in that: a value generated from said intermediate value by means of a signature key-applied cryptography process is applied as a collation value for data verification.

42. The data verifying value imparting method according to Claim 41, characterized in that: different signature keys are applied to the cryptography process for said intermediate integrity check value depending on a localization of said content data, to obtain the collation value for data verification.

43. The data verifying value imparting method according to Claim 42, characterized in that: a common signature key common to all entities of a system for executing a data verifying process or an apparatus-specific signature key specific to each apparatus that executes a data verifying process is selected and used as said signature key depending on the localization of the content data.

44. The data verifying value imparting method according to Claim 36, characterized in that:

said partial integrity check value contains one or more header section integrity check values for in intra-header-section data partly constituting data and one or more content integrity check values for intra-content-section data partly constituting the data, and

said method is set so that a general integrity check value is generated for all said header section integrity check values and said content integrity check values, to verify the data.

45. The data verifying value imparting method according to Claim 36, characterized in that:

said partial integrity check value contains one or more header section integrity check values for intra-header-section data partly constituting data, and

said method is set so that a general integrity check value is generated for said one or more header section integrity check values and content block data partly constituting said data, to verify the data.

46. A program providing medium for providing a computer program for causing a data verifying process to be executed on a computer system to verify that data are valid, the program providing medium being characterized in that said computer program comprises steps of:

executing a collation process using partial integrity check values generated as integrity check values for a partial data set containing one or more partial data obtained by dividing data a plurality of parts, and

using an intermediate integrity check value based on a partial integrity check value set obtained by combining a plurality of said partial integrity check values together, to verify the entirety of a plurality of partial data sets corresponding to the plurality of partial integrity check values constituting said partial integrity check value set.

47. A data processing apparatus comprising:

an encryption processing section that executes encryption processing of at least one of data encryption, data decryption,

data verification, authentication processing and signature processing; and

a storage section that stores master keys to generate keys used for said encryption processing,

characterized in that said encryption processing section is configured to generate individual keys necessary to execute said encryption processing based on said master keys, an encryption processing target apparatus or data identification data.

48. The data processing apparatus according to Claim 47, characterized in that said data processing apparatus is a data processing apparatus that performs encryption processing on transfer data via a storage medium or communication medium,

said storage section stores a distribution key generation master key MKdis for generating a distribution key Kdis used for encryption processing of said transfer data, and

said encryption processing section executes encryption processing based on the distribution key generation master key MKdis stored in said storage section and a data identifier, which is identification data of said transfer data and generates said transfer data distribution key Kdis.

49. The data processing apparatus according to Claim 47, characterized in that said data processing apparatus is a data

processing apparatus that performs authentication processing of an externally connected apparatus to/from which data is transferred,

said storage section stores an authentication key generation master key MKake for generating an authentication key Kake of said externally connected apparatus, and

said encryption processing section executes encryption processing based on the authentication key generation master key MKake stored in said storage section and an externally connected apparatus identifier, which is identification data of said externally connected apparatus and generates the authentication key Kake of said externally connected apparatus.

50. The data processing apparatus according to Claim 47, characterized in that said data processing apparatus is a data processing apparatus that performs signature processing on data,

said storage section stores a signature key generation master key MKdev for generating a data processing apparatus signature key Kdev of said data processing apparatus, and

said encryption processing section executes encryption processing based on the signature key generation master key MKdev stored in said storage section and a data processing apparatus identifier, which is identification data of said data processing apparatus and generates the data processing apparatus signature key Kdev of said data processing apparatus.

51. The data processing apparatus according to Claim 47, characterized in that individual key generation processing that generates an individual key necessary to execute encryption processing based on said master key and identification data of the apparatus or data subject to encryption processing is encryption processing that uses at least part of identification data of the apparatus or data subject to encryption processing as a message and applies said master key as the encryption key.

52. The data processing apparatus according to Claim 51, characterized in that said encryption processing is encryption processing using a DES algorithm.

53. A data processing system configured by a plurality of data processing apparatuses, characterized in that each of said plurality of data processing apparatuses having a common master key to generate a key used for encryption processing of at least one of data encryption, data decryption data verification, authentication processing and signature processing, and

each of said plurality of data processing apparatuses generating a common individual key necessary to execute said encryption processing based on said master key and identification data of the apparatus or data subject to encryption processing.

54. The data processing system according to Claim 53, characterized in that said plurality of data processing apparatuses is configured by a contents data providing apparatus that supplies contents data and a contents data utilization apparatus that utilizes the contents data,

both the contents data providing apparatus and contents data utilization apparatus have a distribution key generation master key to generate a contents data distribution key used for encryption processing of circulation contents data between said contents data providing apparatus and contents data utilization apparatus,

said contents data providing apparatus generates a contents data distribution key based on said distribution key generation master key and contents identifier, which is an identifier of supplied contents data and executes encryption processing on said contents data, and

said contents data utilization apparatus generates a contents data distribution key based on said distribution key generation master key and contents identifier, which is an identifier of supplied contents data and executes decryption processing on said contents data.

55. The data processing system according to Claim 54, characterized in that said contents data providing apparatus has a plurality of different distribution key generation master keys to

generate a plurality of different contents data distribution keys, generates a plurality of different contents data distribution keys based on said plurality of distribution key generation master keys and said contents identifier, executes encryption processing using said plurality of distribution keys generated and generates encryption contents data of a plurality of types, and

said contents data utilization apparatus has at least one distribution key generation master key of the plurality of different distribution key generation master keys owned by said contents data providing apparatus and makes decodable only encryption contents data by a distribution key generated using the same distribution key generation master key as the distribution key generation master key owned by the own apparatus.

56. The data processing system according to Claim 53, characterized in that each of said plurality of data processing apparatuses stores a same contents key generation master key to generate a contents key used for encryption processing of contents data,

data processing apparatus A, which is one of said plurality of data processing apparatuses, stores contents data encrypted by a contents key generated based on said contents key generation master key and the apparatus identifier of said data processing apparatus A in a storage medium,

different data processing apparatus B generates a contents key based on said same contents key generation master key and the apparatus identifier of said data processing apparatus A and executes decryption processing on the encrypted contents data stored by said data processing apparatus A in said storage medium based on said contents key generated.

57. The data processing system according to Claim 53, characterized in that said plurality of data processing apparatuses are configured by a host device and a slave device subject to authentication processing by said host device,

both said host device and said slave device have an authentication key generation master used for authentication processing between the host device and slave device,

said slave device generates an authentication key based on said authentication key generation master key and said slave device identifier, which is the identifier of said slave device and stores in memory in the slave device, and

said host device generates an authentication key based on said authentication key generation master key and the slave device identifier, which is the identifier of said slave device and executes authentication processing.

58. A data processing method that executes encryption processing of at least one of data encryption, data decryption, data

verification, authentication processing and signature processing, comprising:

a key generating step of generating individual keys necessary to execute encryption processing based on master keys to generate the key used for said encryption processing and identification data of the apparatus or data subject to encryption processing; and

an encryption processing step of executing encryption processing based on the key generated in said key generating step.

59. The data processing method according to Claim 58, characterized in that data processing executed by said data processing method is encryption processing on transfer data via a storage medium or communication medium,

said key generating step is a distribution key generating step of executing encryption processing based on a distribution key generation master key MKdis for generating a distribution key Kdis used for encryption processing of transfer data and a data identifier, which is identification data of said transfer data, and generating distribution key Kdis of said transfer data, and

said encryption processing step is a step of executing encryption processing on transfer data based on the distribution key Kdis generated in said distribution key generating step.

60. The data processing method according to Claim 58, characterized in that data processing executed by said data processing method is authentication processing of an externally connected apparatus to/from which data is transferred,

said key generating step is an authentication key generating step of executing encryption processing based on an authentication key generation master key MKake for generating an authentication key Kake of said externally connected apparatus and an externally connected apparatus identifier, which is identification data of said externally connected apparatus, and generating said authentication key Kake of said externally connected apparatus, and

said encryption processing step is a step of executing authentication processing of the externally connected apparatus based on the authentication key Kake generated in said authentication key generating step.

61. The data processing method according to Claim 58, characterized in that data processing executed by said data processing apparatus is signature processing on data,

said key generating step is a signature key generating step of executing encryption processing based on a signature key generation master key MKdev for generating a data processing apparatus signature key Kdev of said data processing apparatus and a data processing apparatus identifier, which is identification

data of said data processing apparatus and generating the data processing apparatus signature key Kdev of said data processing apparatus, and

said encryption processing step is a step of executing signature processing on data based on the signature key Kdev generated in said signature key generating step.

62. The data processing method according to Claim 58, characterized in that said key generating step is encryption processing that uses at least part of data identification of the apparatus or data subject to encryption processing as a message and applies said master key as the encryption key.

63. The data processing method according to Claim 62, characterized in that said encryption processing is encryption processing using a DES algorithm.

64. A data processing method in a data processing system comprising:

a contents data providing apparatus that supplies contents data; and

a contents data utilization apparatus that utilizes the contents data, characterized in that

said contents data providing apparatus generates a contents data distribution key based on a distribution key generation

master key for generating a contents data distribution key used for encryption processing on contents data and a contents identifier, which is the identifier of the provided contents data and executes encryption processing on said contents data, and

said contents data utilization apparatus generates a contents data distribution key based on said distribution key generation master key and a contents identifier, which is the identifier of the provided contents data and executes decryption processing on said contents data.

65. The data processing method according to Claim 64, characterized in that said contents data providing apparatus has a plurality of different distribution key generation master keys to generate a plurality of different contents data distribution keys, generates a plurality of different contents data distribution keys based on said plurality of distribution key generation master keys and said contents identifier, executes encryption processing using said plurality of distribution keys generated and generates encryption contents data of a plurality of types, and

said contents data utilization apparatus has at least one distribution key generation master key of the plurality of different distribution key generation master keys owned by said contents data providing apparatus and decrypts only encryption contents data by a distribution key generated using the same

distribution key generation master key as the distribution key generation master key owned by the own apparatus.

66. A data processing method in a data processing system configured by a plurality of data processing apparatuses comprising:

a step of storing, by data processing apparatus A, which is one of said plurality of data processing apparatuses, in a storage medium contents data encrypted using a contents key generated based on a contents key generation master key to generate a contents key used for encryption processing of contents data and the apparatus identifier of said data processing apparatus A;

a step of generating the same contents key as said contents key by different data processing apparatus B based on the same said contents key generation master key as that of said data processing apparatus A and the apparatus identifier of said data processing apparatus A; and

a step of decrypting the contents data stored in said storage medium using the contents key generated by said data processing apparatus B.

67. A data processing method in a data processing system comprising:

a host device; and

a slave device subject to authentication processing by said host device, characterized in that

said slave device generates an authentication key based on an authentication key generation master key to generate an authentication key used for authentication processing between the host device and slave device and a slave device identifier, which is the identifier of said slave device and stores the authentication key generated in memory in said slave device, and

said host device generates an authentication key based on said authentication key generation master key and slave device identifier, which is the identifier of said slave device and executes authentication processing.

68. A program providing medium that supplies a computer program to execute encryption processing of at least one of data encryption, data decryption, data verification, authentication processing and signature processing on a computer system, said computer program comprising:

a key generating step of generating individual keys necessary to execute said encryption processing based on said master keys to generate the keys used for said encryption processing and identification data of the apparatus or data subject to encryption processing; and

an encryption processing step of executing encryption processing based on the keys generated in said key generating step.

69. A data processing apparatus that processes contents data supplied from a storage medium or communication medium, comprising:

a storage section that stores data processing apparatus identifiers;

a list verification section that extracts an illegal device list included in the contents data and executes collation between entries of said list and said data processing apparatus identifiers stored in said storage section; and

a control section that stops executing processing of at least either one of reproduction of said contents data or processing of storage in a recording device when the result of the collation processing in said collation processing section shows that said illegal device list includes information that matches said data processing identifiers.

70. The data processing apparatus according to Claim 69, characterized in that said list verification section comprises an encryption processing section that executes encryption processing on said contents data; and

said encryption processing section verifies the presence or absence of tampering in said illegal device list based on check values of the illegal device list included in said contents data

and executes said collation processing only when said verification proves no tampering.

71. The data processing apparatus according to Claim 70, further comprising an illegal device list check value generation key, characterized in that said encryption processing section executes encryption processing applying said illegal device list check value generation key to illegal device list configuration data to be verified, generates illegal device list check values, executes collation between said illegal device list check values and the illegal device list check values included in said contents data and thereby verifies the presence or absence of tampering in said illegal device list.

72. The data processing apparatus according to Claim 69, characterized in that

said list verification section comprises an encryption processing section that executes encryption processing on said contents data; and

said encryption processing section executes decryption processing of the encrypted illegal device list included in said contents data and executes said collation processing on the illegal device list resulting from said decryption processing.

73. The data processing apparatus according to Claim 69, characterized in that

said list verification section comprises an encryption processing section that executes mutual authentication processing with a recording device to/from which contents data is transferred; and

said list verification section extracts the illegal device list included in said contents data and executes collation with said data processing apparatus identifiers stored in said storage section on condition that authentication with said recording device has been established through mutual authentication processing executed by said encryption processing section.

74. A data processing method that processes contents data supplied from a storage medium or communication medium, comprising:

a list extracting step of extracting an illegal device list included in the content data;

a collation processing step of executing collation between entries included in the list extracted in said list extracting step and said data processing apparatus identifiers stored in a storage section in the data processing apparatus; and

a step of stopping execution of processing of at least either one of reproduction of said contents data or processing of storage in a recording device when the result of the collation processing

in said collation processing step shows that said illegal device list includes information that matches said data processing identifiers.

75. The data processing method according to Claim 74, further comprising a verification step of verifying the presence or absence of tampering in said illegal device list based on check values of the illegal device list included in said contents data,

characterized in that said collation processing step executes collation processing only when said verification step proves no tampering.

76. The data processing method according to Claim 75, characterized in that said verification step comprising:

a step of executing encryption processing applying an illegal device list check value generation key to illegal device list configuration data to be verified and generating illegal device list check values; and

a step of executing collation between the illegal device list check values generated and the illegal device list check values included in said contents data and thereby verifying the presence or absence of tampering in said illegal device list.

77. The data processing method according to Claim 74, further comprising a decrypting step of executing decrypting processing on the encrypted illegal device list included in said contents data,

characterized in that said collation processing step executes said collation processing on the illegal device list resulting from said decrypting step.

78. The data processing method according to Claim 74, further comprising a mutual authentication processing step of executing mutual authentication processing with a recording device to/from which contents data is transferred, characterized in that

said collation processing step executes said collation processing on condition that authentication with said recording device has been established through mutual authentication processing executed in said mutual authentication processing step.

79. A contents data generation method that generates contents data supplied from a storage medium or communication medium to a plurality of recorders/reproducers, characterized in that an illegal device list whose component data comprises identifiers of recorders/reproducers, which will be excluded from the use of said contents data is stored as the header information of the contents data.

80. The contents data generation method according to Claim 79, characterized in that illegal device list check values for a tampering check on said illegal device list are stored as the header information of the contents data.

81. The contents data generation method according to Claim 79, characterized in that said illegal device list is encrypted and stored in the header information of the contents data.

82. A program supply medium that supplies a computer program that allows a computer system to execute processing of contents data supplied from a storage medium or communication medium, said computer program comprising:

a list extracting step of extracting an illegal device list included in the contents data;

a collation processing step of executing collation between entries included in the list extracted in said list extracting step and said data processing apparatus identifiers stored in a storage section in the data processing apparatus; and

a step of stopping execution of processing of either one of reproduction of said contents data or processing of storage in a recording device when the result of the collation processing in said collation processing step shows that said illegal device list includes information that matches said data processing identifiers.

83. A data processing apparatus that processes contents data supplied via a recording medium or communication medium, comprising:

an encryption processing section that executes encryption processing on said contents data;

a control section that executes control over said encryption processing section;

a system common key used for encryption processing in said encryption processing section, which is common to other data processing apparatuses using said contents data; and

at least one of an apparatus-specific key, which is specific to the data processing apparatus used for encryption processing in said encryption processing section or an apparatus-specific identifier to generate said apparatus-specific key, characterized in that

said encryption processing section is configured to perform encryption processing by applying either one of said system common key or said apparatus-specific key according to the utilization mode of said contents data.

84. The data processing apparatus according to Claim 83, characterized in that said encryption processing section executes encryption processing by applying either one of said system common key or said apparatus-specific key according to utilization restriction information included in said contents data.

85. The data processing apparatus according to Claim 83, further comprising a recording device for recording contents data, characterized in that

said encryption processing section, when imposed with a utilization restriction that said contents data should be used only for the own data processing apparatus, generates data to be stored in said recording device by executing encryption processing using said apparatus-specific key for said contents data; and

in the case where said contents data is also made available to an apparatus other than the own data processing apparatus, data to be stored in said recording device is generated by executing encryption processing using said system common key on said contents data.

86. The data processing apparatus according to Claim 83, comprising a signature key Kdev specific to the data processing apparatus and a system signature key Ksys common to a plurality of data processing apparatuses, characterized in that

said encryption processing section, when said contents data is stored in said recording device imposed with a utilization restriction that said contents data should be used only for the own data processing apparatus, generates an apparatus-specific check value through encryption processing applying said apparatus-specific signature key Kdev to said contents data and, when said

contents data is stored in said recording device with said contents data also made available to an apparatus other than the own data processing apparatus, generates an overall check value through encryption processing applying said system signature key Ksys to said contents data; and

said control section performs control of storing either one of said apparatus-specific check value generated by said encryption processing section or said overall check value together with said contents data in said recording device.

87. The data processing apparatus according to Claim 83, comprising a signature key Kdev specific to the data processing apparatus and a system signature key Ksys common to a plurality of data processing apparatuses, characterized in that

said encryption processing section, when contents data imposed with a utilization restriction that said contents data should be used only for the own data processing apparatus is reproduced, generates an apparatus-specific check value applying said apparatus-specific signature key Kdev to said contents data and executes collation processing on said apparatus-specific check value generated and, when contents data also made available to an apparatus other than the own data processing apparatus is reproduced, generates an overall check value through encryption processing applying said system signature key Ksys to said

contents data and performs collation processing on said overall check value generated; and

said control section generates reproducible decrypted data by continuing processing of contents data by the encryption processing section only when collation with said apparatus-specific check value is established or when collation with said overall check value is established.

88. The data processing apparatus according to Claim 83, comprising a recording data processing apparatus signature key master key MKdev and data processing apparatus identifier IDdev, characterized in that

said encryption processing section generates a signature key Kdev as the data processing apparatus specific key through encryption processing based on said data processing apparatus signature key master key MKdev and said data processing apparatus identifier IDdev.

89. The data processing apparatus according to Claim 88, characterized in that said encryption processing section generates said signature key Kdev through DES encryption processing applying said data processing apparatus signature key master key MKdev to said data processing apparatus identifier IDdev.

90. The data processing apparatus according to Claim 83, characterized in that said encryption processing section generates an intermediate integrity check value by executing encryption processing on said contents data and executes encryption processing applying said data processing apparatus specific key or system common key to said intermediate integrity check value.

91. The data processing apparatus according to Claim 90, characterized in that said encryption processing section generates a partial integrity check value through encryption processing on a partial data set containing at least one partial data item obtained by dividing said contents data into a plurality of parts and generates an intermediate integrity check value through encryption processing on a partial integrity check value set data string containing said partial integrity check value generated.

92. A data processing method that processes contents data supplied via a recording medium or communication medium, characterized by selecting either one of an encryption processing system common key common to other data processing apparatuses using said contents data or an apparatus-specific key, which is specific to the data processing apparatus according to the utilization mode of said contents data; and

executing encryption processing by applying the selected encryption processing key to said contents data.

93. The data processing method according to Claim 92, characterized in that said encryption processing key selecting step is a step of selecting according to utilization restriction information contained in said contents data.

94. The data processing method according to Claim 92, characterized in that the processing of storing contents data in the recording device, when imposed with a utilization restriction that said contents data should be used only for the own data processing apparatus, generates data to be stored in said recording device by executing encryption processing applying said apparatus-specific key to said contents data; and

in the case where said contents data is also made available to an apparatus other than the own data processing apparatus, data to be stored in said recording device is generated by executing encryption processing using said system common key on said contents data.

95. The data processing method according to Claim 92, characterized in that when said contents data is stored in said recording device imposed with a utilization restriction that said contents data should be used only for the own data processing apparatus, the processing of recording contents data in the recording device generates an apparatus-specific check value

through encryption processing applying said apparatus-specific signature key Kdev to said contents data and, when said contents data is stored in said recording device with said contents data also made available to an apparatus other than the own data processing apparatus, generates an overall check value through encryption processing applying said system signature key Ksys to said contents data; and

either one of said apparatus-specific check value generated or said overall check value is stored together with said contents data in said recording device.

96. The data processing method according to Claim 92, characterized in that when contents data imposed with a utilization restriction that said contents data should be used only for the own data processing apparatus is reproduced, the contents data reproducing processing generates an apparatus-specific check value through encryption processing applying said apparatus-specific signature key Kdev to said contents data and executes collation processing on said apparatus-specific check value generated and, when contents data imposed with a utilization restriction that the contents data is also made available to an apparatus other than the own data processing apparatus is reproduced, generates an overall check value through encryption processing applying said system signature key Ksys to said

contents data and performs collation processing on said overall check value generated; and

contents data is reproduced only when collation with said apparatus-specific check value is established or when collation with said overall check value is established.

97. The data processing method according to Claim 92, further comprising a step of generating a signature key Kdev as the data processing apparatus specific key through encryption processing based on data processing apparatus signature key master key MKdev and data processing apparatus identifier IDdev.

98. The data processing method according to Claim 97, characterized in that said signature key Kdev generating step is a step of generating said signature key Kdev through DES encryption processing applying said data processing apparatus signature key master key MKdev to said data processing apparatus identifier IDdev.

99. The data processing method according to Claim 92, further comprising a step of generating an intermediate integrity check value by executing encryption processing on said contents data, characterized by executing encryption processing applying said data processing apparatus specific key or system common key to said intermediate integrity check value.

100. The data processing method according to Claim 99, characterized by further generating a partial integrity check value through encryption processing on a partial data set containing at least one partial data item obtained by dividing said contents data into a plurality of parts and generating an intermediate integrity check value through encryption processing on a partial integrity check value set data string containing said partial integrity check value generated.

101. A program supply medium that supplies a computer program allowing a computer system to execute data processing that processes contents data supplied via a recording medium or communication medium, said computer program comprising the steps of:

selecting either encryption processing key, an encryption processing system common key common to other data processing apparatuses using said contents data or an apparatus-specific key, which is specific to the data processing apparatus according to the utilization mode of said contents data; and

executing encryption processing applying the selected encryption processing key to said contents data.

102. A data processing apparatus that processes contents data supplied via a recording medium or communication medium, comprising:

an encryption processing section that executes encryption processing on said contents data; and

a control section that executes control over said encryption processing section, characterized in that

said encryption processing section is configured to generate a contents check value in units of contents block data to be verified included in the data, execute collation on the contents check value generated and thereby execute verification processing on the validity of each contents block data in said data.

103. The data processing apparatus according to Claim 102, comprising a contents check value generation key, characterized in that said encryption processing section generates a contents intermediate value based on contents block data to be verified and generate a contents check value by executing encryption processing applying said contents check value generation key to said contents intermediate value.

104. The data processing apparatus according to Claim 103, characterized in that when the contents block data to be verified is encrypted, said encryption processing section generates a contents intermediate value by executing predetermined operation

processing on an entire decrypted statement obtained through decryption processing of said contents block data in units of a predetermined number of bytes, and when the contents block data to be verified is not encrypted, generates a contents intermediate value by executing predetermined operation processing on the entire contents block data in units of a predetermined number of bytes.

105. The data processing apparatus according to Claim 104, characterized in that said predetermined operation processing applied in said intermediate integrity check value generation processing by said encryption processing section is an exclusive-OR operation.

106. The data processing apparatus according to Claim 104, characterized in that said encryption processing section has an encryption processing configuration in CBC mode and said decryption processing applied to the content intermediate value generation processing when the contents block data to be verified is decryption processing in CBC mode.

107. The data processing apparatus according to Claim 106, characterized in that the encryption processing configuration in CBC mode of said encryption processing section is a configuration

in which common key encryption processing is applied a plurality of times only to part of a message string to be processed.

108. The data processing apparatus according to Claim 102, characterized in that when the contents block data contains a plurality of parts and some parts included in said contents block data are to be verified, said encryption processing section generates a contents check value based on the parts to be verified, executes collation processing on the contents check value generated and thereby executes verification processing on the validity in units of content block data in said data.

109. The data processing apparatus according to Claim 108, characterized in that when said contents block data contains a plurality of parts and it is one part that needs to be verified, said encryption processing section generates a contents check value by executing encryption processing applying the contents check value generation key to a value obtained by carrying out an exclusive-OR in units of a predetermined number of bytes on the entire decrypted statement obtained by decryption processing of parts to be verified in the case where said parts to be verified is encrypted, and generates a contents check value by executing encryption processing applying said contents check value generation key to a value obtained by carrying out an exclusive-OR in units of a predetermined number of bytes on said entire part to

be verified in the case where said parts to be verified is not encrypted.

110. The data processing apparatus according to Claim 108, characterized in that when said contents block data contains a plurality of parts and it is a plurality of parts that needs to be verified, said encryption processing section uses, as a contents check value, the result obtained by executing encryption processing applying said contents check value generation key to link data of a parts check value obtained by executing encryption processing applying a contents check value generation key to each part.

111. The data processing apparatus according to Claim 102, characterized in that said encryption processing section further comprises a recording device for storing contents data containing contents block data whose validity has been verified.

112. The data processing apparatus according to Claim 111, characterized in that when collation is not established in the collation processing on a contents check value in said encryption processing section, said control section stops storage in said recording device.

113. The data processing apparatus according to Claim 102, characterized in that said encryption processing section further comprises a reproduction processing section for reproducing data whose validity has been verified.

114. The data processing apparatus according to Claim 113, characterized in that when collation is not established in the collation processing on a contents check value in said encryption processing section, said control section stops reproduction processing in said reproduction processing section.

115. A data processing method that processes contents data supplied via a recording medium or communication medium, characterized by generating a contents check value in units of contents block data to be verified included in the data, executing collation on the contents check value generated and thereby executing verification processing on the validity in units of contents block data in said data.

116. The data processing method according to Claim 115, characterized by generating a contents intermediate value based on contents block data to be verified and generating a contents check value by executing encryption processing applying said contents check value generation key to said contents intermediate value generated.

117. The data processing method according to Claim 115, characterized by generating, when the contents block data to be verified is encrypted, a contents intermediate value by executing predetermined operation processing on an entire decrypted statement obtained through decryption processing of said contents block data in units of a predetermined number of bytes, and generating, when the contents block data to be verified is not encrypted, a contents intermediate value by executing predetermined operation processing on the entire contents block data in units of a predetermined number of bytes.

118. The data processing method according to Claim 117, characterized in that said predetermined operation processing applied in said intermediate integrity check value generation processing is an exclusive-OR operation.

119. The data processing method according to Claim 117, characterized in that in said contents intermediate value generation processing, said decryption processing applied to the content intermediate value generation processing when the contents block data to be verified is encrypted is decryption processing in CBC mode.

120. The data processing method according to Claim 119, characterized in that in said decryption processing configuration in CBC mode, common key encryption processing is applied a plurality of times only to part of a message string to be processed.

121. The data processing method according to Claim 115, characterized by generating, when the contents block data contains a plurality of parts and some parts included in said contents block data are to be verified, a contents check value based on the parts to be verified, executing collation processing on the contents check value generated and thereby executing verification processing on the validity in units of content block data in said data.

122. The data processing method according to Claim 121, characterized by generating, when the contents block data contains a plurality of parts and it is one part that needs to be verified, a contents check value by executing encryption processing applying the contents check value generation key to a value obtained by carrying out an exclusive-OR in units of a predetermined number of bytes on the entire decrypted statement obtained by decryption processing of parts to be verified in the case where said part to be verified is encrypted, and generating a contents check value by executing encryption processing applying said contents check value

generation key to a value obtained by carrying out an exclusive-OR in units of a predetermined number of bytes on said entire part to be verified in the case where said part to be verified is not encrypted.

123. The data processing method according to Claim 121, characterized by using, when said contents block data contains a plurality of parts and it is a plurality of parts that needs to be verified, as a contents check value, the result obtained by executing encryption processing further applying said contents check value generation key to link data of a parts check value obtained by executing encryption processing applying the contents check value generation key to each part.

124. The data processing method according to Claim 115, further comprising a step of storing contents data containing contents block data whose validity has been verified.

125. The data processing method according to Claim 124, characterized in that when collation is not established in the collation processing on a contents check value, said control section stops storage in said recording device.

126. The data processing method according to Claim 115, further comprising a step of reproducing data whose validity has been verified.

127. The data processing method according to Claim 126, characterized by stopping reproduction processing when collation is not established in the collation processing on a contents check value.

128. A contents data verification value assignment method for contents data verification processing, characterized by generating a contents check value in units of contents block data to be verified included in the data, assigning the contents check value generated to contents data containing the contents block data to be verified.

129. The contents data verification value assignment method according to Claim 128, characterized in that said contents check value is generated through encryption processing applying the contents check value generation key using the contents block data to be checked as a message.

130. The contents data verification value assignment method according to Claim 128, characterized in that said contents check

value is generated by generating a contents intermediate value based on the contents block data to be verified and executing encryption processing applying said contents check value generation key to said contents intermediate value.

131. The contents data verification value assignment method according to Claim 128, characterized in that said contents check value is generated by executing encryption processing in CBC mode on the contents block data to be verified.

132. The contents data verification value assignment method according to Claim 131, characterized in that said encryption processing configuration in CBC mode is a configuration in which common key encryption processing is applied a plurality of times only to part of a message string to be processed.

133. The contents data verification value assignment method according to Claim 128, characterized by generating, when the contents block data contains a plurality of parts and some parts included in said contents block data are to be verified, a contents check value based on the parts to be verified and assigning the contents check value generated to contents data containing the content block data to be verified.

134. The contents data verification value assignment method according to Claim 133, characterized by generating, when said contents block data contains a plurality of parts and it is one part that needs to be verified, a contents check value by executing encryption processing applying the contents check value generation key to a value obtained by carrying out an exclusive-OR in units of a predetermined number of bytes on the entire decrypted statement obtained by decryption processing of parts to be verified in the case where said parts to be verified is encrypted, generating a contents check value by executing encryption processing applying said contents check value generation key to a value obtained by carrying out an exclusive-OR in units of a predetermined number of bytes on said entire part to be verified in the case where said parts to be verified is not encrypted and assigning the contents check value generated to the contents data containing the contents block data to be verified.

135. The contents data verification value assignment method according to Claim 133, characterized by using, when said contents block data contains a plurality of parts and it is a plurality of parts that needs to be verified, as a contents check value, the result obtained by executing encryption processing further applying said contents check value generation key to link data of a parts check value obtained by executing encryption processing applying the contents check value generation key to each part and

assigning the contents check value generated to contents data containing the contents block data to be verified.

136. A program supply medium that supplies a computer program to execute data processing on contents data supplied via a recording medium or communication medium, said computer program comprising:

a step of generating a contents check value in units of contents block data to be verified included in the data; and

a step of executing collation processing on the contents check value generated and thereby executing verification processing on the validity in units of contents block data in said data.

137. A data processing apparatus for executing processing for generating storing data with respect to a recording device of content data, which has a plurality of content blocks in which at least a part of the blocks are encrypted and a header section storing information on the contents blocks, characterized in that:

in the case in which content data to be an object of storage in said recording device is structured by data stored in said header section, which is an encryption key data Kdis[Kcon] that is an encryption key Kcon of said content block applied encryption processing by an encryption key Kdis,

said data processing apparatus has a structure for executing processing for taking out said encryption key data Kdis[Kcon] from

said header section and executing decryption processing to generate decryption data Kcon, generating a new encryption key data Kstr[Kcon] that is applied encryption processing by an encryption key Kstr and storing the new encryption key data Kstr[Kcon] in the header section of said content data, and applying a different encryption key Kstr to the generated decryption data Kcon to execute decryption processing.

138. A data processing apparatus for executing processing for generating storing data with respect to a recording device of content data, which has a plurality of content blocks in which at least a part of the blocks are encrypted and a header section storing information on the contents blocks, characterized in that:

in the case in which said content block included in content data to be an object of storage with respect to said recording device is composed of contents encrypted by an encryption key Kblc and encryption key data Kcon[Kblc] that is encrypted by the encryption key Kcon, and has a structure in which encryption key data Kdis[Kcon] that is the encryption key Kcon applied encryption processing by an encryption key Kdis is stored in said header section,

said data processing apparatus has a structure for executing processing for taking out said encryption key data Kdis[Kcon] from said header section and executing decryption processing to generate decryption data Kcon, generating a new encryption key

data Kstr[Kcon] that is applied encryption processing by an encryption key Kstr and storing the encryption key data Kstr[Kcon] in the header section of said content data, and applying a different encryption key Kstr to the generated decryption data Kcon to execute decryption processing.

139. A data processing apparatus for executing processing for generating storing data with respect to a recording device of content data, which has a plurality of content blocks in which at least a part of the blocks are encrypted and a header section storing information on the contents blocks, characterized in that:

in the case in which said content block included in content data to be an object of storage with respect to said recording device is composed of contents encrypted by an encryption key Kblc and encryption key data Kdis[Kblc] that is encrypted by the encryption key Kdis,

said data processing apparatus has a structure for executing processing for taking out said encryption key data Kdis[Kblc] from said content block section and executing decryption processing of the encryption key Kblc to generate decryption data Kblc, generating an encryption key data Kstr[Kblc] that is applied encryption processing by an encryption key Kstr and storing the encryption key data Kstr[Kblc] in a contents block section, and applying a different encryption key Kstr to the generated decryption data Kblc to execute decryption processing.

140. A content data generating method for generating content data, comprising:

coupling a plurality of content blocks composed of data including at least any one of voice information, image information and program data;

applying encryption processing to at least a part of content blocks included in said plurality of content blocks by an encryption key Kcon;

generating encryption key data Kdis[Kcon] that is said encryption key Kcon applied encryption processing by an encryption key Kdis and storing the encryption key Kdis in a header section of said content data; and

generating content data including said plurality of content blocks and the header section.

141. The content data generating method according to Claim 140, characterized in that said content data generating method further comprises processing of:

generating block information that stores information including;

identification information on content data;

usage policy information including a data length of the content data and a data type of the content data; and

information including a data length of said content block and presence or absence of encryption processing, and

storing the information in said header section.

142. The content data generating method according to Claim 140, characterized in that said content data generating method further comprises processing of:

generating a part check value based on a part of information composing said header section and storing the part check value in said header section; and

generating a total check value based on said part check value and storing the total check value in said header section.

143. The content data generating method according to Claim 142, characterized in that generation processing of said part check value and generation processing of said total check value are executed by applying a DES encryption processing algorithm with data to be an object of check as a message and a check value generation key as an encryption key.

144. The content data generating method according to Claim 141, characterized in that said content data generating method further comprises:

applying encryption processing to said block information by the encryption key Kbit and storing the encryption key data

Kdis[Kbit] that is the encryption key Kbit generated by the encryption key Kdis in said header section.

145. The content data generating method according to Claim 140, characterized in that each block of a plurality of blocks in said content block is generated as a common fixed data length.

146. The content data generating method according to Claim 140, characterized in that each block of a plurality of blocks in said content block is generated as a configuration in which an encryption data section and a non-encryption data section are arranged regularly.

147. A content data generating method for generating content data comprising:

coupling a plurality of content blocks including at least any one of voice information, image information and program data;

composing at least a part of the plurality of content blocks by an encryption data section that is data including at least any one of voice information, image information and program data by an encryption key Kblc, and a set of encryption key data Kcon[Kblc] that is the encryption key Kblc of the encryption data section applied encryption processing by an encryption key Kcon;

generating encryption key data Kdis[Kcon] that is the encryption key Kcon applied encryption processing by an encryption

key Kdis and storing the generated the encryption key data Kdis[Kcon] in a header section of said content data; and

generating content data including a plurality of content blocks and a header section.

148. A content data generating method for generating content data comprising:

coupling a plurality of content blocks including at least any one of voice information, image information and program data;

composing at least a part of the plurality of content blocks by an encryption data section that is data including at least any one of voice information, image information and program data by an encryption key Kblc, and a set of encryption key data Kdis[Kblc] that is the encryption key Kblc of the encryption data section applied encryption processing by an encryption key Kdis; and

generating content data including a plurality of content blocks and a header section.

149. A data processing method for executing processing for storing in a recording device of content data having a plurality of content blocks in which at least a part of blocks are encrypted, and a header section in which information on the content blocks is stored, comprising:

in the case in which content data to be an object of storage in said recording device is structured by data stored in said

header section, which is an encryption key data Kdis[Kcon] that is an encryption key Kcon of said content block applied encryption processing by an encryption key Kdis,

taking out said encryption key data Kdis[Kcon] from said header section and executing decryption processing to generate decryption data Kcon;

generating a new encryption key data Kstr[Kcon] that is applied encryption processing by an encryption key Kstr by applying a different encryption key Kstr to the generated decryption data Kcon to execute encryption processing; and

storing said generated encryption key data Kstr[Kcon] in a header section of said content data, and storing the header section in said recording device together with said plurality of content blocks.

150. A data processing method for executing processing for storing in a recording device of content data having a plurality of content blocks in which at least a part of blocks are encrypted, and a header section in which information on the content blocks is stored, comprising:

in the case in which said content block included in content data to be an object of storage with respect to said recording device is composed of contents encrypted by an encryption key Kblc and encryption key data Kcon[Kblc] that is encrypted by the encryption key Kcon, and has a structure in which encryption key

data Kdis[Kcon] that is the encryption key Kcon applied encryption processing by an encryption key Kdis is stored in said header section,

taking out said encryption key data Kdis[Kcon] from said header section and executing decryption processing to generate decryption data Kcon;

generating a new encryption key data Kstr[Kcon] that is applied encryption processing by an encryption key Kstr by applying a different encryption key Kstr to the generated decryption data Kcon to execute encryption processing; and

storing said generated encryption key data Kstr[Kcon] in a header section of said content data, and storing the header section in said recording device together with said plurality of content blocks.

151. A data processing method for executing processing for storing in a recording device of content data having a plurality of content blocks in which at least a part of blocks are encrypted, and a header section in which information on the content blocks is stored, comprising:

in the case in which said content block included in content data to be an object of storage with respect to said recording device is composed of contents encrypted by an encryption key Kblc and encryption key data Kdis[Kblc] that is encrypted by the encryption key Kdis,

taking out said encryption key data Kdis[Kblc] from said content block section and executing decryption processing of the encryption key Kblc to generate decryption data Kblc;

generating an encryption key data Kstr[Kblc] that is applied encryption processing by an encryption key Kstr by applying a different encryption key Kstr to the generated decryption data Kblc to execute encryption processing; and

storing said generated encryption key data Kstr[Kblc] in a content block section, and storing the content block section in said recording device together with said plurality of content blocks.

152. A program providing medium for providing a computer program causing generation processing of storing data with respect to a recording device of content data, which has a plurality of content blocks in which at least a part of the blocks are encrypted and a header section storing information on the contents blocks, to be executed on a computer system, characterized in that:

said computer program comprises:

in the case in which content data to be an object of storage in said recording device is structured by data stored in said header section, which is an encryption key data Kdis[Kcon] that is an encryption key Kcon of said content block applied encryption processing by an encryption key Kdis,

a step of taking out said encryption key data Kdis[Kcon] from said header section and executing decryption processing to generate decryption data Kcon;

generating a new encryption key data Kstr[Kcon] that is applied encryption processing by an encryption key Kstr by applying a different encryption key Kstr to the generated decryption data Kcon to execute encryption processing; and

storing said generated encryption key data Kstr[Kcon] in a header section of said content data.

153. A data processing apparatus for performing reproduction processing of content data provided by a storage medium or a communication medium, characterized by comprising:

a content data analyzing section for executing content data analysis of content data including compressed contents and an expansion processing program of said compressed contents, and executing extraction processing of the compressed contents and the expansion processing program from said content data; and

an expansion processing section for executing expansion processing of the content data included in said content data using an expansion processing program included in the content data obtained as a result of the analysis of said content data analyzing section.

154. The data processing apparatus according to Claim 153, characterized by further comprising:

a data storing section for storing the compressed contents that are extracted by said content data analyzing section; and

a program storing section for storing the expansion processing program extracted by said content data analyzing section, and characterized in that said expansion processing section has a configuration for executing expansion processing with respect to the compressed contents stored in said data storing section by applying the expansion processing program stored in said program storing section to the compressed contents.

155. The data processing apparatus according to Claim 153, characterized in that said contents data analyzing section has a configuration for obtaining a configuration information of content data based on header information included in said content data and performing analysis of the content data.

156. The data processing apparatus according to Claim 155, characterized in that reproduction priority information of the compressed contents is included in said header information and, if there are a plurality of compressed contents that is objects of expansion processing in said expansion processing section, said expansion processing section has a configuration for sequentially executing content expansion processing in accordance with the

priority based on the priority information in the header information obtained in said content data analyzing section.

157. The data processing apparatus according to Claim 153, characterized by further comprising:

displaying means for displaying information of the compressed contents that are objects of expansion processing; and

inputting means for inputting reproduction contents identification data selected from the content information displayed on said displaying means, and characterized in that said expansion processing section has a configuration for executing expansion processing of the compressed contents corresponding to the identification data based on the reproduction contents identification data inputted from said inputting means.

158. A data processing apparatus for performing reproduction processing of content data provided by a storage medium or a communication medium, characterized by comprising:

a content data analyzing section for receiving content data including either compressed contents or expansion processing program, distinguishing whether the content data has the compressed contents or the expansion processing program from header information included in the received content data and, at the same time, if the content data has the compressed contents, obtaining a type of a compressing processing program applied to

the compressed contents from the header information of the content data, and if the content data has the expansion processing program, obtaining a type of the expansion processing program from the header information of the content data;

an expansion processing section for executing expansion processing of the compressed contents, characterized in that said expansion processing section has a configuration for selecting an expansion processing program applicable to the type of the compression processing program of the compressed contents analyzed by said content data analyzing section based on the type of the expansion processing program analyzed by said content data analyzing section, and executing expansion processing by the selected expansion processing program.

159. The data processing apparatus according to Claim 158, characterized by further comprising:

a data storing section for storing the compressed contents that are extracted by said content data analyzing section; and

a program storing section for storing the expansion processing program extracted by said content data analyzing section, and characterized in that said expansion processing section has a configuration for executing expansion processing with respect to the compressed contents stored in said data storing section by applying the expansion processing program stored in said program storing section to the compressed contents.

160. The data processing apparatus according to Claim 158, characterized in that reproduction priority information of the compressed contents is included in said header information and, if there are a plurality of compressed contents that is objects of expansion processing, content expansion processing in said expansion processing section has a configuration for sequentially executing content expansion processing in accordance with the priority based on the priority information in the header information obtained in said content data analyzing section.

161. The data processing apparatus according to Claim 158, characterized by further comprising retrieving means for retrieving an expansion processing program, and characterized in that said retrieving means has a configuration for retrieving an expansion processing program applicable to a type of the compression processing program of the compressed contents analyzed by said content data analyzing section with program storing means accessible by said data processing apparatus as an object of retrieval.

162. The data processing apparatus according to Claim 158, characterized by further comprising:

displaying means for displaying information of the compressed contents that are objects of expansion processing; and

inputting means for inputting reproduction contents identification data selected from the content information displayed on said displaying means, and characterized in that said expansion processing section has a configuration for executing expansion processing of the compressed contents corresponding to the identification data based on the reproduction contents identification data inputted from said inputting means.

163. A data processing method for performing reproduction processing of content data provided by a storage medium or a communication medium, characterized by comprising:

a content data analyzing step of executing content data analysis of content data including compressed contents and an expansion processing program of said compressed contents, and executing extraction processing of the compressed contents and the expansion processing program from said content data; and

an expansion processing step of executing expansion processing of the compressed content included in said content data using an expansion processing program included in the content data obtained as a result of the analysis of said content data analyzing step.

164. The data processing method according to Claim 163, characterized by further comprising:

a data storing step of storing the compressed contents that are extracted by said content data analyzing step; and

a program storing step of storing the expansion processing program extracted by said content data analyzing section, and characterized in that said expansion processing section has a configuration for executing expansion processing with respect to the compressed contents stored in said data storing step by applying the expansion processing program stored in said program storing step to the compressed contents.

165. The data processing method according to Claim 163, characterized in that said contents data analyzing step obtains a configuration information of content data based on header information included in said content data and performs analysis of the content data.

166. The data processing method according to Claim 165, characterized in that reproduction priority information of the compressed contents is included in said header information and, if there are a plurality of compressed contents that is objects of expansion processing in said expansion processing section, said expansion processing step sequentially executes content expansion processing in accordance with the priority based on the priority information in the header information obtained in said content data analyzing step.

167. The data processing method according to Claim 163, characterized by further comprising:

displaying step of displaying information of the compressed contents that are objects of expansion processing on displaying means; and

inputting step of inputting reproduction contents identification data selected from the content information displayed on said displaying means, and characterized in that said expansion processing step executes expansion processing of the compressed contents corresponding to the identification data based on the reproduction contents identification data inputted from said inputting step.

168. A data processing method for performing reproduction processing of content data provided by a storage medium or a communication medium, characterized by comprising:

a content data analyzing step of receiving content data including either compressed contents or expansion processing program, distinguishing whether the content data has the compressed contents or the expansion processing program from header information included in the received content data and, at the same time, if the content data has the compressed contents, obtaining a type of a compressing processing program applied to the compressed contents from the header information of the content

data, and if the content data has the expansion processing program, obtaining a type of the expansion processing program from the header information of the content data;

a selecting step of selecting an expansion processing program applicable to the type of the compression processing program of the compressed contents analyzed in said content data analyzing step based on the type of the expansion processing program analyzed in said content data analyzing step; and

an expansion processing step of executing expansion processing by the expansion processing program selected in said selecting step.

169. The data processing method according to Claim 168, characterized by further comprising:

a data storing step of storing the compressed contents that are extracted by said content data analyzing section; and

a program storing step of storing the expansion processing program extracted by said content data analyzing section, and characterized in that said expansion processing step executes expansion processing with respect to the compressed contents stored in said data storing step by applying the expansion processing program stored in said program storing step to the compressed contents.

170. The data processing method according to Claim 168, characterized in that reproduction priority information of the compressed contents is included in said header information and, if there are a plurality of compressed contents that is objects of expansion processing, said content expansion processing step sequentially executes content expansion processing in accordance with the priority based on the priority information in the header information obtained in said content data analyzing step.

171. The data processing method according to Claim 168, characterized by comprising a retrieving step of retrieving an expansion processing program, and characterized in that said retrieving step retrieves an expansion processing program applicable to a type of the compression processing program of the compressed contents analyzed in said content data analyzing step with program storing means accessible by said data processing apparatus as an object of retrieval.

172. The data processing method according to Claim 168, characterized by further comprising:

a displaying step of displaying on displaying means information of the compressed contents that are objects of expansion processing; and

an inputting step of inputting reproduction contents identification data selected from the content information

displayed on said displaying means, and characterized in that said expansion processing step executes expansion processing of the compressed contents corresponding to the identification data based on the reproduction contents identification data inputted from said inputting means.

173. A content data generating method for performing generation processing of content data provided by a storage medium or a communication medium, characterized by generating content data in which compressed contents and an expansion processing program of the compressed contents are combined.

174. The content data generating method according to Claim 173, characterized in that a configuration information of the content data is added as header information of said content data.

175. The content data generating method according to Claim 173, characterized in that reproduction priority information of contents included in the content data as header information of the content data.

176. A content data generating method for performing generation processing of content data provided by a storage medium or a communication medium, characterized in that content data is generated in which a type of content data for identifying whether

the content data has compressed contents or an expansion processing program is added as header information;

if the content data has compressed contents, a type of a compression processing program applied to the compressed contents is added as header information; and

if the content data has an expansion processing program, a type of an expansion processing program is added as header information.

177. The content data generating method according to Claim 176, characterized in that reproduction priority information of contents included in the content data is added as header information of said content data.

178. A program providing medium for providing a computer program that causes a computer system to execute reproduction processing of content data provided by a storage medium or a communication medium, characterized by comprising:

a content data analyzing step of executing content data analysis of content data including compressed contents and an expansion processing program of said compressed contents, and executing extraction processing of the compressed contents and the expansion processing program from said content data; and

an expansion processing step of executing expansion processing of the content data included in said content data using

an expansion processing program included in the content data obtained as a result of the analysis of said content data analyzing section.